REMARKS

This application has been carefully reviewed in light of the Office Action dated October 22, 2007. Applicant has amended claims 1 and 14 and cancelled claims 12-13. Reconsideration and favorable action in this case are respectfully requested.

The Examiner has rejected claims 1-11 and 14-21 under 35 U.S.C. §102(b) as being unpatentable over EP 0843249 to Helmut. Applicants have reviewed this reference in detail and do not believe that it discloses or makes obvious the invention as claimed.

As stated in the previous Amendment, the device shown in Helmut works in a different manner and yields different results than the present invention. The cryptographic unit (CU) provides a set of services to the host system (p. 11, lines 21-24). For an application to use the CU, the application must first be installed. A certified application includes an application image 29 and a certificate 28 from the ADA (application domain authority). The certificate includes application ID 137 and a class of service 136 defined for the application. Using these two elements, the CU produces a "credential" 130 which identifies the application (a name or a hash value of the application image) and the class of service defined by the application (p. 13, lines 39-51). The credential is signed by the CU (application signature 138). Assuming that the application signature identifies the particular CU, which is certainly not clear from the Helmut specification, the only certificate that could bind the particular CU with the application is the credential 130. Hence, under this assumption, the application is bound to the particular CU, by the CU itself.

The purpose of the credential is to ensure that an application has authority to access a CU and that it is not modified during operation. The authority to access a CU appears to extend to all CUs, not any particular CU.

The present invention performs an entirely different function. Only firmware (or, alternatively, application software or data) approved by the manufacturer can be used to control the computing device and the firmware cannot be replaced or modified by someone other than the manufacturer. This prevents alteration of the operation of the computing device by third party modifications (i.e., viruses) or by user changes to the device's intended settings.

In the Helmut device, the application software is not initially uniquely associated to a particular CU – the association, if it occurs at all, is generated by the CU itself. The only result of the association is that, once installation occurs, the application cannot be changed. But there is no disclosure in Helmut that the same certified application could not be used with another host and CU, *because there is no unique association between the application and the CU or the application and the host.* There is no disclosure in Helmut to suggest that a given application can be used on one and only own host, or that it could access one and only one CU.

In the Response to Arguments, the Examiner states that Helmut discloses binding by the manufacturer at page 7, lines 46-48. The portion of Helmut states:

> The second method has additional applicability for software copyright schemes. Sending the application in encrypted form to the target side and letting the CU decrypt the program does not only reveal that the CU is a valid CU, but also allows the software manufacturer to send out an application tailored to that particular CU, i.e. host system. *Unfortunately, once decrypted the application image is available in the clear and can be copied to other systems with little or no effort.* [emphasis added]

This portion of Helmut is part of the larger description in Helmut of "CU Validation", i.e., the process of ensuring that the application requesting cryptographic services is assured about the identity of the CU. The "second method" described in the above-quoted portion is "Challenge the CU", by issuing a puzzle that only the CU can resolve. In sending an encrypted application to the CU and asking the CU to decrypt it, the application would know that the CU had the stated decryption ability. But there is no disclosure that the CU is the only CU that could decrypt the application file. Nor is the encrypted program of Helmut an association between an electronic file (i.e., the encrypted application file) and *an identifier* linked to the computing device (i.e., the host or CU). Further, the association between the application program and the identifier is specified to be in a digital certificate – merely sending a encrypted program would not constitute a digital certificate containing information uniquely associating the electronic file and the identifier linked to the computing device.

The quoted paragraph itself states that once decrypted the application image is available in the clear and can be copied to other systems with little or no effort. Thus, the application image file is not uniquely associated with an identifier linked to the CU or the host system. If the application image were uniquely associated with an identifier on either the host or the CU, and if the processing system would only access the application image if there was a valid association between the current state of the application image and the identifier, then the statement in the last sentence of the quoted paragraph could not be true.

What is clear from the quoted paragraph is: (1) there is no digital certificate uniquely associating an electronic file with an identifier linked to the computing device – if there were one, there would be no need to decrypt the program to prove that the CU was in fact a valid CU and (2) nothing prevents either the host or the CU from accessing the program prior to determining a unique association – since both the CU and the host have explicit access to the encrypted application file.

Therefore, Applicants respectfully request allowance of independent claims 1 and 14. Further, Applicants request allowance of dependent claims 2-11 and 15-21.

The Commissioner is hereby authorized to charge any fees or credit any overpayment, including extension fees, to Deposit Account No. 20-0668 of Texas Instruments Incorporated.

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Alan W. Lintel, Applicants' Attorney at (972) 664-9595 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

/Alan W. Lintel/

Alan W. Lintel
Attorney for Applicant(s)
Reg. No. 32478

January 22, 2008
Anderson, Levine & Lintel
14785 Preston Rd.
Suite 650
Dallas, Texas 75254
Tel. (972) 664-9595